

Vector-Circulant Matrices over Finite Fields and Related Codes

Somphong Jitman

Abstract

A vector-circulant matrix is a natural generalization of the classical circulant matrix and has applications in constructing additive codes. This article formulates the concept of a vector-circulant matrix over finite fields and gives an algebraic characterization for this kind of matrix. Finally, a construction of additive codes with vector-circulant based over \mathbb{F}_4 is given together with some examples of good half-rate additive codes.

1 Introduction

Let q be a power of a prime number and n be a positive integer. Denote by \mathbb{F}_q the finite field of order q and $M_n(\mathbb{F}_q)$ the \mathbb{F}_q -algebra of all $n \times n$ matrices whose entries are in \mathbb{F}_q . Given $\alpha \in \mathbb{F}_q \setminus \{0\}$, a matrix $A \in M_n(\mathbb{F}_q)$ is said to be α -*twistulant* [3] if

$$A = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ \alpha a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ \alpha a_{n-2} & \alpha a_{n-1} & \dots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha a_1 & \alpha a_2 & \dots & \alpha a_{n-1} & a_0 \end{bmatrix}.$$

Such a matrix is called *circulant* [resp., *negacirculant*] *matrix* when $\alpha = 1$ [resp., $\alpha = -1$]. The set of all $n \times n$ circulant [resp., α -twistulant, negacirculant] matrices over \mathbb{F}_q is isomorphic to $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ [resp., $\mathbb{F}_q[x]/\langle x^n - \alpha \rangle$, $\mathbb{F}_q[x]/\langle x^n + 1 \rangle$] as commutative algebras [3].

Circulant matrices over finite fields and their well-known generalizations in the notion of twistulant and negacirculant matrices have widely been applied in many branches of Mathematics. Recently, they have been applied to construct circulant based additive codes [5] and double circulant codes [4] with optimal and extremal parameters.

In Section 2, we generalize the concept of circulant matrix over the finite field \mathbb{F}_q and call it a vector-circulant matrix. The algebraic structure of the set of these matrices is investigated. This generalization leads to a construction of vector-circulant based additive codes over \mathbb{F}_4 in Section 3. Examples are some optimal codes are also demonstrated here.

2 Vector-Circulant Matrices over Finite Fields

Given a vector $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_{n-1}) \in \mathbb{F}_q^n$, let $\rho_\lambda : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ be defined by

$$\begin{aligned} \rho_\lambda((v_0, v_1, \dots, v_{n-1})) &= (0, v_0, v_1, \dots, v_{n-2}) + v_{n-1}\lambda \\ &= (v_{n-1}\lambda_0, v_0 + v_{n-1}\lambda_1, \dots, v_{n-2} + v_{n-1}\lambda_{n-1}). \end{aligned} \quad (2.1)$$

S. Jitman is with the Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand (email: sjitman@gmail.com).

The map ρ_{λ} is called the λ -vector-cyclic shift on \mathbb{F}_q^n .

A matrix $A \in M_n(\mathbb{F}_q)$ is said to be *vector-circulant*, or specifically, λ -vector-circulant if

$$A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ \rho_{\lambda}(a_0) & a_1 & \cdots & a_{n-1} \\ \rho_{\lambda}^2(a_0) & a_1 & \cdots & a_{n-1} \\ \vdots & & & \\ \rho_{\lambda}^{n-1}(a_0) & a_1 & \cdots & a_{n-1} \end{bmatrix} =: \text{cir}_{\lambda}(a_0, a_1, \dots, a_{n-1}).$$

Clearly, a λ -vector-circulant matrix becomes the classical circulant [resp., α -twistualnt] matrix when λ is the vector $(1, 0, \dots, 0)$ [resp, $(\alpha, 0, \dots, 0)$].

Example 2.1. Consider the finite field $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$. The matrices

$$\begin{bmatrix} 1 & \alpha & 0 \\ 0 & 1 & \alpha \\ \alpha & 0 & \alpha^2 \end{bmatrix} = \text{cir}_{(1,0,1)}(1, \alpha, 0)$$

and

$$\begin{bmatrix} 1 & \alpha & 0 & \alpha \\ \alpha^2 & 1 & \alpha & \alpha \\ \alpha^2 & \alpha & 1 & 0 \\ 0 & \alpha^2 & \alpha & 1 \end{bmatrix} = \text{cir}_{(\alpha,0,0,1)}(1, \alpha, 0, \alpha)$$

are 3×3 and 4×4 vector-circulant matrices, respectively. They are obviously not circulant.

From (2.1), it is easily verified that ρ_{λ} is an \mathbb{F}_q -linear transformation corresponding to

$$T_{\lambda} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \lambda_0 & \lambda_1 & \lambda_2 & \cdots & \lambda_{n-1} \end{bmatrix},$$

i.e., $\rho_{\lambda}(\mathbf{v}) = \mathbf{v}T_{\lambda}$, for all $\mathbf{v} \in \mathbb{F}_q^n$. Consequently, for $1 \leq i$, ρ_{λ}^i is an \mathbb{F}_q -linear transformation corresponding to T_{λ}^i . Hence,

$$\text{cir}_{\lambda}(a_0, a_1, \dots, a_{n-1}) = \sum_{i=0}^{n-1} a_i \text{cir}_{\lambda}(E_{i+1}), \quad (2.2)$$

where $E_i = (0, \dots, 0, \underbrace{1}_{i^{th}}, 0, \dots, 0)$, for $1 \leq i \leq n$.

Observe that T_{λ} need not be invertible. For $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_{n-1})$, the singularity of T_{λ} depends on λ_0 . By applying a suitable sequence of elementary row operations, T_{λ} is equivalent to an $n \times n$ diagonal matrix $\text{diag}(\lambda_0, 1, 1, \dots, 1)$. Then the next proposition follows.

Proposition 2.2. $T_{(\lambda_0, \lambda_1, \dots, \lambda_{n-1})}$ is invertible if and only if $\lambda_0 \neq 0$.

The set of all $n \times n$ λ -vector-circulant matrices over \mathbb{F}_q is denoted by $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$. Consider $M_n(\mathbb{F}_q)$ as an algebra over \mathbb{F}_q , our goal is to show that $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$ is an abelian subalgebra of $M_n(\mathbb{F}_q)$. It follows directly from the linearity of ρ_{λ} that $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$ is a subspace of the \mathbb{F}_q -vector space $M_n(\mathbb{F}_q)$. Moreover, by application of (2.1), the set $\{\text{cir}_{\lambda}(E_1), \text{cir}_{\lambda}(E_2), \dots, \text{cir}_{\lambda}(E_n)\}$ can be verified to be a basis of $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$. To prove that $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$ is a commutative ring, we need the following lemma and corollary. For convenience, let T_{λ}^0 denote the identity matrix I_n .

Lemma 2.3. *i) $T_{\lambda}^m = \text{cir}_{\lambda}(\rho_{\lambda}^m(E_1))$, for all integers $0 \leq m$.*

ii) $T_{\lambda}^i = \text{cir}_{\lambda}(E_{i+1})$, for all $0 \leq i < n$.

Proof. First, we prove *i)* by induction on m . By the definition, $T_{\lambda}^0 = I_n = \text{cir}_{\lambda}(\rho_{\lambda}^0(E_1))$. Clearly, $T_{\lambda} = \text{cir}_{\lambda}(\rho_{\lambda}(E_1))$. Assume that $T_{\lambda}^k = \text{cir}_{\lambda}(\rho_{\lambda}^k(E_1))$ for all positive integers $k < m$. Then

$$\begin{aligned} T_{\lambda}^{k+1} &= \text{cir}_{\lambda}(\rho_{\lambda}^k(E_1))T_{\lambda} \\ &= \begin{bmatrix} \rho_{\lambda}^k(E_1) \\ \rho_{\lambda}^{k+1}(E_1) \\ \vdots \\ \rho_{\lambda}^{k+n-1}(E_1) \end{bmatrix} T_{\lambda} \\ &= \begin{bmatrix} \rho_{\lambda}^{k+1}(E_1) \\ \rho_{\lambda}^{k+2}(E_1) \\ \vdots \\ \rho_{\lambda}^{k+n}(E_1) \end{bmatrix} \\ &= \text{cir}_{\lambda}(\rho_{\lambda}^{k+1}(E_1)). \end{aligned}$$

Hence *i)* is proved.

Note that, for all $1 \leq i \leq n$, $\rho_{\lambda}^{i-1}(E_1) = E_i$. Hence, *ii)* follows immediately from *i)*. \square

The next corollary is a direct consequence of Lemma 2.3.

Corollary 2.4. $T_{\lambda}^m \in \text{Cir}_{n,\lambda}(\mathbb{F}_q)$, for all $0 \leq m$.

Theorem 2.5. $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$ is a commutative subring of $M_n(\mathbb{F}_q)$.

Proof. Since $(\text{Cir}_{n,\lambda}(\mathbb{F}_q), +)$ is an additive subgroup of $M_n(\mathbb{F}_q)$ containing $I_n = T_{\lambda}^0$, it is sufficient to show that $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$ is closed under the usual multiplication of matrices. Let $(a_0, a_1, \dots, a_{n-1})$, $(b_0, b_1, \dots, b_{n-1}) \in \mathbb{F}_q^n$. Then

$$\begin{aligned} \text{cir}_{\lambda}(a_0, a_1, \dots, a_{n-1}) \text{cir}_{\lambda}(b_0, b_1, \dots, b_{n-1}) &= \left(\sum_{i=0}^{n-1} a_i \text{cir}_{\lambda}(E_{i+1}) \right) \left(\sum_{j=0}^{n-1} b_j \text{cir}_{\lambda}(E_{j+1}) \right), \\ &\quad \text{by (2.2),} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j \text{cir}_{\lambda}(E_{i+1}) \text{cir}_{\lambda}(E_{j+1}) \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j T^i T^j, \quad \text{by Lemma 2.3,} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j T^{i+j} \\ &\in \text{Cir}_{n,\lambda}(\mathbb{F}_q), \quad \text{by Corollary 2.4.} \end{aligned} \tag{2.3}$$

From (2.3), the commutativity is obvious. \square

Corollary 2.6. $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$ is a commutative algebra.

Proof. It follows from the fact that $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$ is an \mathbb{F}_q -vector space and Theorem 2.5. \square

For $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_{n-1})$, let $\lambda(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_{n-1} x^{n-1}$ be the corresponding polynomial representation of λ .

The next theorem is an algebraic characterization of $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$.

Theorem 2.7. $\text{Cir}_{n,\lambda}(\mathbb{F}_q)$ is isomorphic to $\mathbb{F}_q[x]/\langle x^n - \lambda(x) \rangle$ as commutative algebras.

Proof. Defined $\varphi : \text{Cir}_{n,\lambda}(\mathbb{F}_q) \rightarrow \mathbb{F}_q[x]/\langle x^n - \lambda(x) \rangle$ by

$$\text{cir}_{\lambda}(a_0, a_1, \dots, a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i x^i + \langle x^n - \lambda(x) \rangle.$$

It is easily seen that φ is an additive group isomorphism. Let $(a_0, a_1, \dots, a_{n-1}), (b_0, b_1, \dots, b_{n-1}) \in \mathbb{F}_q^n$ and $\alpha \in \mathbb{F}_q$. Then

$$\begin{aligned} \varphi(\alpha \text{cir}_{\lambda}(a_0, a_1, \dots, a_{n-1})) &= \varphi(\text{cir}_{\lambda}(\alpha a_0, \alpha a_1, \dots, \alpha a_{n-1})) \\ &= \sum_{i=0}^{n-1} \alpha a_i x^i + \langle x^n - \lambda(x) \rangle \\ &= \alpha \left(\sum_{i=0}^{n-1} a_i x^i + \langle x^n - \lambda(x) \rangle \right) \\ &= \alpha \varphi(\text{cir}_{\lambda}(a_0, a_1, \dots, a_{n-1})). \end{aligned} \tag{2.4}$$

By (2.3) and Lemma 2.3, we then have

$$\begin{aligned} &\varphi(\text{cir}_{\lambda}(a_0, a_1, \dots, a_{n-1}) \text{cir}_{\lambda}(b_0, b_1, \dots, b_{n-1})) \\ &= \varphi\left(\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j T^{i+j}\right), \quad \text{by (2.3),} \\ &= \varphi\left(\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j \text{cir}_{\lambda}(\rho_{\lambda}^{i+j}(E_1))\right), \quad \text{by Lemma 2.3,} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j \varphi(\text{cir}_{\lambda}(\rho_{\lambda}^{i+j}(E_1))), \quad \text{by (2.4),} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j x^{i+j} + \langle x^n - \lambda(x) \rangle \\ &= \left(\sum_{i=0}^{n-1} a_i x^i + \langle x^n - \lambda(x) \rangle \right) \left(\sum_{j=0}^{n-1} a_j x^j + \langle x^n - \lambda(x) \rangle \right) \\ &= \varphi(\text{cir}_{\lambda}(a_0, a_1, \dots, a_{n-1})) \varphi(\text{cir}_{\lambda}(b_0, b_1, \dots, b_{n-1})). \end{aligned}$$

This completes the proof. \square

3 Vector-Circulant Based Additive Codes over \mathbb{F}_4

In this section, we restrict our study to the finite field of 4 elements $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$. A code of length n over \mathbb{F}_4 is defined to be a non-empty subset of \mathbb{F}_4^n . A code C is said to be additive if it is an additive subgroup of the additive group $(\mathbb{F}_4^n, +)$. Throughout, every code is assume to be additive. It is know [5] that C contains 2^k codewords for some $0 \leq k \leq 2n$, and can be defined by a $k \times n$ generator matrix, with entries from \mathbb{F}_4 , whose rows span C additively. We regard an additive code of length n over \mathbb{F}_4 containing 2^k codewords as an $(n, 2^k)$ code. The Hamming weight of $v \in \mathbb{F}_4^n$, denoted $\text{wt}(v)$, is defined to be the number of nonzero components of v . The Hamming distance between $u \neq v \in \mathbb{F}_4^n$ is defined as $\text{wt}(u - v)$. The minimum distance of the code C , denoted by $d(C)$, is the minimal Hamming distance between any two distinct codewords of C . As C is additive, the minimum distance equals the smallest nonzero weight of any codewords in C . An $(n, 2^k)$ code with minimum distance d is called an $(n, 2^k, d)$ code.

We focus on a construction of additive codes for the particular case $k = n$, or half-rate codes, or equivalently, $(n, 2^n)$ codes. It follows from the Singleton bound [2] that any half-rate additive code over \mathbb{F}_4 must satisfy

$$d \leq \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

An $(n, 2^n)$ code C is said to be *extremal* if it attains the equality in the Singleton bound, and *near-extremal* if it has minimum distance $\lfloor \frac{n}{2} \rfloor$.

Given $\lambda \in \mathbb{F}_4^n$, a λ -*vector-circulant based additive code* is defined to be an additive code generated by a λ -circulant generator matrix of the following form:

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ \rho_\lambda(a_0) & a_1 & \cdots & a_{n-1} \\ \rho_\lambda^2(a_0) & a_1 & \cdots & a_{n-1} \\ \vdots & & & \\ \rho_\lambda^{n-1}(a_0) & a_1 & \cdots & a_{n-1} \end{bmatrix} =: \text{cir}_\lambda(a_0, a_1, \dots, a_{n-1})$$

Such a code is called a circulant based additive code if $\lambda = (1, 0, \dots, 0)$ and it is called a α -twistulant based additive code if $\lambda = (\alpha, 0, \dots, 0)$.

An advantage of this construction is that there are typically much more additive codes than circulant based or twistulant based additive codes [5].

We implement a procedure in the computer algebra system Magma [1] to construct vector-circulant based additive codes. Based on this construction, we search for half-rate additive codes with highest minimum distances of length up to 13. The result is shown in Table 1; codes of length 2 to 7 are extremal and codes of length 8 to 13 are near-extremal.

References

- [1] Bosma W, Cannon J J, Playoust C. The Magma algebra system I: the user language. *Journal of Symbolic Computation*, **24**: 235–265 (1997)
- [2] Danielsen L E, Parker M G. Directed graph representation of half-rate additive codes over $\text{GF}(4)$. <http://arxiv.org/abs/0902.3883v3> (preprint)
- [3] Davis P J. *Circulant Matrices*. Chelsea publishing, New York, second edition, 1994
- [4] Grassl M, Gulliver A. On circulant self-dual codes over small fields. *Designs, Codes and Cryptography*, **52**: 57–81 (2009)
- [5] Gulliver T A, Kim J-L. Circulant based extremal additive self-dual codes over $\text{GF}(4)$. *IEEE Transaction on Information Theory*, **50**: 359–366 (2004)

Table 1: Vector-circulant based $(n, 2^n)$ codes C over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$ generated by $\text{cir}_\lambda(v)$ with highest minimum distances

n	λ	v	$d(C)$
2	(1, 1)	$(\alpha, 1)$	2
3	(1, 0, α)	$(\alpha, 1, 1)$	2
4	(1, 0, 0, 1)	$(1, \alpha, 1, 1)$	3
5	(1, 0, 0, 0, α)	$(1, 0, \alpha, 1, 1)$	3
6	(1, 0, 0, 0, 0, 0)	$(\alpha, \alpha^2, \alpha, 1, 1, 1)$	4
7	(1, 0, 1, 0, 0, 0, 0)	$(0, 1, \alpha, 1, 1, 1, 1)$	4
8	(1, 0, 0, 0, 0, 0, 0, α)	$(0, \alpha, \alpha^2, \alpha^2, 1, 1, 1, 1)$	4
9	(1, 0, 0, 0, 0, 0, 0, 0, 1)	$(\alpha^2, \alpha, 1, 1, 1, 1, 1, 1, 1)$	4
10	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0)	$(0, \alpha, \alpha, 1, \alpha, 1, 1, 1, 1, 1)$	5
11	(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)	$(0, \alpha, \alpha^2, \alpha, 1, 1, 1, 1, 1, 1, 1)$	5
12	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	$(0, 1, \alpha^2, \alpha^2, 1, \alpha, 1, 1, 1, 1, 1, 1)$	6
13	(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	$(0, \alpha, \alpha^2, 1, 1, \alpha, 1, 1, 1, 1, 1, 1, 1)$	6